Amendments to the Specification:

Please replace the paragraph beginning at page 2, line 7 with the following amended paragraph:

Private network 30 ~~20~~ includes an access control policy server 38 that manages an access policy for private network 30 ~~20~~. The various computers and devices included in private network 30 ~~20~~ use access control lists (ACLs) to determine and control access to the resources of private network 30 ~~20~~. The ACLs used by the computers and devices included in network 30 ~~20~~ are maintained and generated by policy server 38, as will be explained.

Please replace the paragraph beginning at page 7, line 6 with the following amended paragraph:

Please note that before firewall computer 32 translates ("tags") the user access request with the private IP address (via NAT), the access control ACLs, for both application layer computers and network layer devices have already been sent by policy server 38, and installed by the respective computers and network devices of private network 30.

Please replace the paragraph beginning at page 9, line 9 with the following amended paragraph:

ACL Entry A and ACL Entry B correspond to network layer ACL entries that are mapped and generated by policy server 38 for the previous example shown in FIG. 2. In more detail, ACL Entry A is generated to ALLOW access for user requests from source IP address "192.163.3.10" ~~"192.163.8.10"~~ (the private IP address allocated to user 24b by DHCP server 40). ACL Entry A also specifies a destination port of server computer 36b, a TCP protocol designation (the network layer of OSI), a source port corresponding to firewall computer 32 and a destination port corresponding to an application on server computer 36b. ACL Entry B would also be generated along with ACL Entry A. ACL Entry B is generated to DENY access to all user 24b requests to any other server besides server 36b. The `*` character included in ACL Entry B is a wildcard character, and is interpreted as all values allowed by the field in which the wildcard is used. In ACL Entry B, therefore, all user requests from source address "192.163.3.10" ~~"192.163.8.10"~~ and from the source address of firewall computer 32 are denied access to any server system in private network 30.